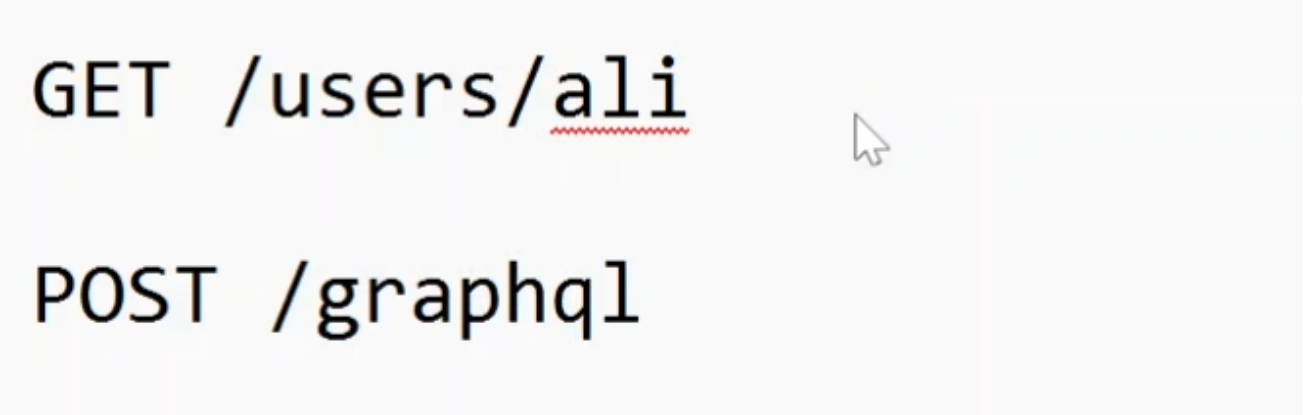
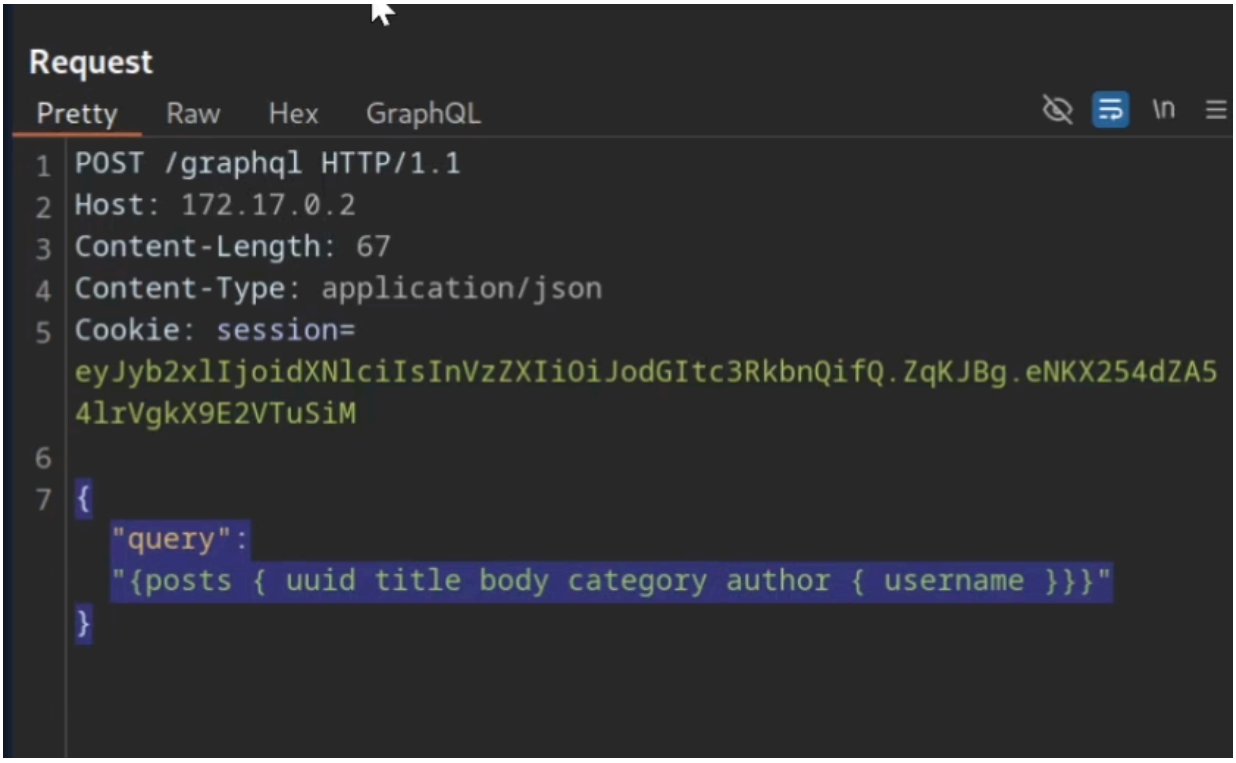
GraphQl

- عباره عن API بيستخرج معلومات عن المستخدم من داخل قواعد البيانات
- الوسيط بين ال FRONT والـ back end
- علشان نشتغل بالـ GraphQl بتتعرف علي two endpoint دايما بيبقي موجود فيهم
  - /graphql
  - /api/graphql
    - لو مش من دول لازم تبقي graphql تبقي موجوده معاه

- 

- الفرق بين الـ Rest API والـ graphql
- ال Rest API
  - بتجيب معلومات عن الـ USER
  - بتغير ف المسار عادي
- الـ GraphQL

- دايما بتستخدم POST والـ graphql ثابته برضو زي كدا



- اللي بيتغير ال body بس

- دا ال payloads اللي بتتحط تحت طلب ال graphql
- بيجيبلك معلومات الـ Users كلهم

- الـ id
- الـ username
- الـ role

```
{
  user(id:1, username:"Hossam") {
    id
    username
    role
  }
}
```

- لو عايز تحدد مش كل الـ Users
- بتشيل حرف ال S
- بتعمل ( ) وتكتب جواهم البيانات اللي عايز تبحث عنها

- اداة graphwOOf بتحددلك السيرفر اللي شغال عليه الـ graphql
- بعد ما تعرف بتخش علي موقع اسمو GraphQl-Threat-matrix وتشوف اي المتاح تشتغل عليه فالسرفر اللي عرفته

---

query IntrospectionQuery { __schema { queryType { name } mutationType { name } subscriptionType { name

- دا الـ introspection اللي بتستخدمه لما بتلاقي graphql دا ثابت
- لو هتستخدمه ف ال burp بتحط قبلهم " query " والكود كلو بيبقي علي سطر واحد
- الـ رد بتاع الكود بتاخده علي موقع اسمو " graphql voyager "

```
{
postByAuthor(author: "htb-stdnt'-- -"){
  uuid
  id
  title
  body
  category
  authorId
}

}
```

- ممكن نستخدم ال SQL Injection
- بتعمل Injection في منطقه الـ User

```
mutation{
  registerUser(input: {username: "hossam", password: "1211111111134"
    {
    user{
      username
      password
      role
      msg
    }
  }
}
```

- بتستخدم الـ mutation بتعدل ف قواعد البيانات